

明 細 書

属性情報提供サーバ、属性情報提供方法、およびプログラム 技術分野

[0001] 本発明は、ネットワークを介して属性情報を提供する属性情報提供サーバ等に関する。

背景技術

[0002] 属性証明書(Attribute Certificate)は、通常の公開鍵証明書が本人性を証明するのに対して、その人物がユーザ権限として、どのような属性を持っているかを証明するものであり、IETF(Internet Engineering Task Force)の定めるX.509でその仕様が定められている(例えば、非特許文献1参照。)。また、発行も公開鍵証明書を発行する公開鍵認証局(Certification Authority)ではなく、属性認証機関(Attribute Authority)によって行われる。このように、本人性と属性との認証を分ける動きは、OASIS(構造化情報標準促進協会)の標準であるSAML(Security Assertion Markup Language)でも取り入れられており、複数の独立機関によるドメインをまたがった柔軟な認証・許可を可能にし、Federated IDという新しい認証サービスの提案にもつながっている(例えば、非特許文献2参照。)。

[0003] この属性情報(属性データ)には、氏名、住所、年齢、職業、電話番号、性別、家族構成などが含まれるが、これらの属性情報の中には、会社の人事部が証明するような組織上の職位に関するようなものから、個人の趣味のようなものまで様々なものがある。前述の属性証明書が使えるものは、属性自身が公的第三者によって証明できるようなものであり、プライバシー保護の観点から、趣味のような個人的な属性には第三者機関を認証機関とするのは適さない。このように、属性には、第三者から認定されるAuthorized属性と、完全に個人の任意で決められるDiscretionary属性があり、それぞれ異なるセキュリティ要件がある。

[0004] ここで、属性データを与信情報として扱うものとして、ICチップ付きのクレジットカード内に、カード番号以外に住所などの属性情報を入れておくことで、商店などにてクレジット決済の際に付加情報を同時に開示できる従来技術が存在する(例えば、特許

文献1参照。)。かかる特許文献1では、付加情報を区分化し、情報の開示レベルによってこの開示する情報をコントロールする機能についても示されている。また、クレジット会社などの運営する信用センターが、各加盟店の信用レベルを格付けし、それによって情報開示レベルを決定する機能についても示されている。

[0005] また、ネットワークを介しての通信における認証システムにて、認証サーバが新規の登録者に対して共通IDであるユニバーサルIDを発行し、このユニバーサルIDを提示した要求に応じて、他の端末者に対して登録者の個人情報から住所などの商取引に必要な情報を抽出して送信することで、ネットワークを介して商品の購入やサービスの提供を受ける際に必要とされる個人情報の入力操作を簡略化する技術が開示されている(例えば、特許文献2参照。)

[0006] 非特許文献1:FC 3281 on An Internet Attribute Certificate[平成15年8月4日検索]インターネット<

<http://www1.ietf.org/mail-archive/ietf-announce/Current/msg18344.html>>

非特許文献2:Liberty Alliance[平成15年8月4日検索]インターネット<

<http://www.projectliberty.org/>>

特許文献1:特開2001-325526号公報(第4-5頁、図1)

特許文献2:特開2001-244927号公報(第3-4頁、図1)

発明の開示

発明が解決しようとする課題

[0007] ところで、前述したAuthorized属性の中で、例えば預金残高や購買履歴、会員情報などといった、個人とそれが属するサービスプロバイダとの共有情報についても、その個人の属性として扱えると便利なが多い。例えば米国においては、カード取得のための審査はかなり厳重で、例えば、1年以上、銀行口座を管理していたという取引履歴が必要とされる。かかる場合に、その取引銀行から認証をしてもらえれば、新規取引が容易となり、加入者にとってもサービスプロバイダにとっても、利のあるサービスとなり得る。こうした共有情報は、本来は個人の情報として保護されるべきものであるが、個人の同意と希望のもとに、かかる情報を、それを保護するサービスプロバイダに認証してもらう個人属性与信サービスの仕組みが望まれるところである。

[0008] また、与信をサービスとするビジネスとしては、クレジットカードが代表的なものであるが、ここでは、与信額を上限とする金銭を与信の対象として、クレジットカード会社の加入者が加入店舗から商品を購入するときの決算サービスが行われている。ところが、インターネットのようなネットワーク上では、お互いに全く知らないもの同士が取引を開始したい場合がある。このようなネットワーク上における与信の特徴として、

1. 与信の対象は金銭以外の信頼情報であること。

2. 取引をしようとする二者は必ずしも同じ信頼機関に属していないこと。

等が挙げられる。そのために、クレジットカードの仕組みでは実現できない、金銭以外で与信になるものとして、信頼できる組織の会員(membership)であることや、その会員として所属する期間、その間の活動履歴などが重要となる。これらは、全て個人とその所属する機関が共有する情報である。また、信頼熟成のためには、取引をしようとしている二者が同じ組織に属している必要はなく、それぞれが備えている基準に照らして、相手を信頼できるかどうか決定できるような仕組みが必要である。現在のクレジットカードの仕組みでは、責任、与信範囲、および取引対象者が予め決められており、こうしたネットワーク上で期待されているようなフレキシブルな与信付与の仕組みは実現されていない。

[0009] 更に、上述した特許文献1に記載の技術では、参加者が従来のクレジットカードの枠組みに制限されており、また、その属性も商店が商品を配送するために必要な情報に限定されている。また、上述したX.509等の属性証明のための技術では、例えば非特許文献1等では属性証明書のフォーマットを決めているだけであり、具体的なサービスの仕組みについてはカバーされていない。また更に、上述した特許文献2に記載の技術では、加入者の匿名性やどの属性を証明するか等について、加入者自身がコントロールすることができない。また、自分がどの新規取引業者と取引しようとしているかを個人情報取り扱い業者に常に認識されることから、加入者にとっては十分なプライバシーの保護が図られない。

[0010] 本発明は、以上のような技術的課題を解決するためになされたものであって、その目的とするところは、インターネットなどのネットワークを用いて、例えば金銭以外の属性を与信の対象とすること等を可能とする属性情報提供サービスを実現することにあ

る。

また他の目的は、加入者の個人情報の一部を、加入者の同意の下で、新規取引者に提供することにある。

更に他の目的は、加入者がどの新規取引業者と取り引きしようとしているかを個人情報取り扱い業者に知られずに、認証を可能とすることにある。

課題を解決するための手段

- [0011] かかる目的のもと、本発明は、属性情報が格納されたデータベースから所定の属性情報をネットワークを介して提供する属性情報提供サーバであって、ネットワークを介して接続されるユーザ装置により、データベースに格納されている属性情報の中から幾つかの属性情報の抜き出し指示を受ける手段と、ユーザ装置によって指示されデータベースから抜き出された幾つかの属性情報だけを仮想レコードとしてデータベースに登録する手段と、仮想レコードのキーとしての仮想IDをユーザ装置に提供する手段と、ネットワークを介して接続される属性情報受信装置から、仮想IDを用いた仮想レコードの読み込み要求を受ける手段と、属性情報受信装置に対して仮想レコードを提供する手段とを含む。
- [0012] ここで、この抜き出し指示を受ける手段は、ユーザ装置だけにユーザ装置の操作者に関する属性情報を参照させ、仮想レコードを抜き出させる際に、任意の属性に対するコピーを許可する一方、任意の属性に対する改ざんを禁止することを特徴とすることができる。これによれば、属性情報提供サーバは、自らがユーザ装置との間で得た活動履歴などの個人情報の一部を、加入者であるユーザ装置の同意の下で、属性情報受信装置に開示する際、それが改ざんされていないということだけを責任範囲として、与信をする仕組みを提供できる。また、読み込み要求を受ける手段は、データベースの中からどの仮想IDに対する仮想レコードの読み込み要求がなされているかを知り得ない状態にあることを特徴とすることができる。
- [0013] 一方、本発明が適用される属性情報提供サーバは、データベースに格納される属性情報の中から選択された所定の情報である仮想レコードを生成手段によって生成し、この仮想レコードのキーとなる仮想IDに対応付けて格納手段によりデータベースに格納する。また、ネットワークを介して接続されるユーザ装置に仮想ID提供手段に

より仮想IDを提供し、ネットワークを介して接続される属性情報受信装置からの仮想IDを用いた要求に基づいて、仮想レコード提供手段は、属性情報受信装置に仮想レコードを提供する。この仮想レコード提供手段は、データベースの中からどの仮想IDが選ばれたかを知り得ない状態にて、属性情報受信装置に仮想レコードを提供することを特徴とすることができる。

[0014] ここで、この生成手段は、データベースに格納されている加入者の属性情報の中から、ユーザ装置によって抜き出された情報を仮想レコードとして生成することを特徴とすることができる。また、この仮想レコード提供手段は、1-out-of-N OT(Oblivious Transfer)のプロトコルを用いて、属性情報受信装置に仮想レコードを提供することを特徴とすることができる。

[0015] 他の観点から捉えると、本発明が適用される属性情報提供サーバは、顧客ごとに、複数の属性情報を含む顧客レコードを格納するデータベースと、顧客が操作するユーザ装置からの要求に基づき、データベースから顧客の顧客レコードを読み出し、ネットワークを介してユーザ装置に提供する顧客レコード表示部と、ユーザ装置からネットワークを介し、顧客レコードの中から所定の属性情報に対する選択を受ける属性選択部と、この属性選択部により受けた選択に基づき、顧客レコードの中から選択された属性情報によって仮想レコードを生成すると共に、生成された仮想レコードをデータベースに格納する仮想レコード生成部と、この仮想レコード生成部により生成された仮想レコードを特定するための仮想IDをユーザ装置に提供する仮想ID発行部と、属性情報受信装置からネットワークを介してなされる仮想IDを用いた情報参照要求に基づき、データベースから該当する仮想レコードを読み出して属性情報受信装置に提供する仮想レコード参照処理部とを含む。

[0016] ここで、この仮想レコード生成部は、オリジナルである顧客レコードの属性内容と、生成された仮想レコードの属性内容とを比較し、改ざんされていないことを検証することを特徴としている。また、この仮想ID発行部によりユーザ装置に提供される仮想IDは、顧客レコードのIDとはアンリカブルなIDであることを特徴とすることができる。

[0017] また、本発明が適用される属性情報提供サーバは、複数の属性情報を含むレコードをレコード格納手段により格納し、このレコード格納手段により格納されたレコード

の中から、ネットワークを介して選択された所定の属性情報によって生成された仮想レコードを仮想レコード格納手段により格納する。そして、どの仮想レコードが選ばれたかを知り得ない状態にて、仮想レコード格納手段の中から選ばれた仮想レコードを、仮想レコード開示手段によりネットワークを介して開示する。

[0018] ここで、この仮想レコード格納手段は、キーとしての仮想IDに対応付けて仮想レコードを格納し、仮想レコード開示手段は、どの仮想IDが選ばれたかを知り得ない状態にて、仮想IDを用いた開示要求を受けることを特徴としている。より具体的には、この仮想レコード開示手段は、オブリビアストランスファー(Oblivious Transfer)の暗号技術を用いて仮想レコードの開示を実現している。

[0019] 一方、本発明を方法のカテゴリから捉えると、本発明が適用される属性情報提供方法は、ネットワークを介してなされたユーザ装置からの要求に基づき、複数の属性情報からなるレコードが格納されたデータベースから、所定のレコードを読み出すステップと、読み出された所定のレコードを、ネットワークを介してユーザ装置に提供するステップと、所定のレコードの中から所定の属性情報に対するユーザ装置からの選択をネットワークを介して受けるステップと、所定のレコードの中から選択された所定の属性情報を含む仮想レコードを生成するステップと、生成された仮想レコードをデータベースに格納するステップと、データベースに格納される仮想レコードの属性情報が顧客レコードの属性情報から改ざんされたものでないことを検証するステップと、格納された仮想レコードを特定するための仮想IDをネットワークを介してユーザ装置に提供するステップと、ネットワークを介して属性情報受信装置から仮想IDを用いた情報参照要求を受けるステップと、この情報参照要求に基づき、データベースから該当する仮想レコードを読み出すステップと、読み出された仮想レコードを属性情報受信装置にネットワークを介して提供するステップと、を含む。この情報参照要求は、1-out-of-N OT(Oblivious Transfer)の Protokol を用いてなされることを特徴とすることができる。

[0020] 更に他の観点から捉えると、本発明が適用される属性情報提供方法は、顧客別の顧客レコードの中から所定の属性が選択されて生成された仮想レコードをキーとなる仮想IDに対応付けて格納されたデータベースに対して、この仮想IDを用いた仮想レ

コードの取得要求を受けるステップと、仮想IDに対応する仮想レコードをデータベースから読み出し、取得要求に対して仮想レコードを開示するステップとを含み、この仮想レコードの取得要求を受けるステップは、取得要求を受ける際に、どの仮想IDが選ばれたかが秘匿されることを特徴としている。ここで、この顧客自身のコンピュータ装置を介して、顧客自身の顧客レコードの中から所定の属性の選択を受けるステップと、選択された所定の属性だけを属性とする仮想レコードを生成してデータベースに格納するステップと、データベースに格納された仮想レコードのキーとなる仮想IDをコンピュータ装置に提供するステップとを更に含むことができる。

[0021] また本発明は、ネットワークを介して属性情報を提供するための属性情報提供サーバとして機能するコンピュータがこれらの各機能を実現可能に構成されたプログラムとして把握することができる。このプログラムをコンピュータに対して提供する際に、例えばサーバとしてのコンピュータにインストールされた状態にて提供される場合の他、コンピュータに実行させるプログラムをコンピュータが読取可能に記憶した記憶媒体にて提供する形態が考えられる。この記憶媒体としては、例えばDVDやCD-ROM媒体等が該当し、DVDやCD-ROM読取装置等によってプログラムが読み取られ、フラッシュROM等にこのプログラムが格納されて実行される。また、これらのプログラムは、例えば、プログラム伝送装置によってネットワークを介して提供される形態がある。

[0022] 具体的には、本発明が適用されるプログラムは、コンピュータに、ネットワークを介してなされたユーザ装置からの要求に基づき、複数の属性情報からなるレコードが格納されたデータベースから、所定のレコードを読み出す機能と、読み出された所定のレコードを、ネットワークを介してユーザ装置に提供する機能と、所定のレコードの中から所定の属性情報に対するユーザ装置からの選択をネットワークを介して受ける機能と、この所定のレコードの中から選択された所定の属性情報を含む仮想レコードを生成する機能と、データベースに格納される仮想レコードの属性情報がレコードの属性情報から改ざんされたものではないことを検証する機能と、生成された仮想レコードをデータベースに格納する機能と、格納された仮想レコードを特定するための仮想IDをネットワークを介してユーザ装置に提供する機能とを実現させる。

- [0023] 他の観点から捉えると、本発明が適用されるプログラムは、ネットワークを介して属性情報を提供するための属性情報提供サーバとして機能するコンピュータに、格納されるレコードの中から所定の属性が選択されて生成された仮想レコードを、キーとなる仮想IDに対応付けてデータベースに格納する機能と、どの仮想IDが選ばれたかが秘匿された状態にて仮想IDを用いた仮想レコードの取得要求を受ける機能と、仮想IDに対応する仮想レコードをデータベースから読み出し、取得要求に対して仮想レコードを開示する機能とを実現させる。

発明の効果

- [0024] 本発明によれば、属性情報を持つ機関が、例えば特定個人の属性情報の一部を第三者に提供することで、例えば特定個人や機関に対して属性情報に関する利益のあるビジネスを提供することができる。

発明を実施するための最良の形態

- [0025] 以下、添付図面を参照して、本発明の実施の形態について詳細に説明する。

図1は、本実施の形態が適用される属性情報提供システム(与信付与システム)の全体構成を示した図である。ここでは、個人情報取り扱い業者に設置される属性情報提供サーバ(個人情報サーバ)10、属性情報提供システムの加入者がクライアント端末として用いるユーザ装置30、新規取引者が利用するクライアント端末である属性情報受信装置(与信情報受信装置)50が配置され、これらがインターネット等のネットワーク70を介して接続されている。このネットワーク70は、インターネットなどの公的、広域的なネットワークでもローカルなネットワークでも良い。すなわち、インターネット上に設けられた公的なデータベースサーバを属性情報提供サーバ10として本実施形態のシステムを構築することもできるし、企業内イントラネットのような閉じた形態で本実施形態のシステムを構築することもできる。

- [0026] サービスプロバイダが管理するサーバである属性情報提供サーバ10は、会員(ユーザ装置30)の個人情報や会員との間の取引情報を管理し、会員の同意に基づいて属性を認証するための仮想IDトークン(VIDトークン)を発行している。仮想IDトークンは、仮想ID(VID)に、例えば属性情報提供サーバ10のURL等を含んで形成される。この仮想IDの発行依頼者として、サービスプロバイダの会員であるユーザ装置3

0では、属性情報提供サーバ10に登録してある個人情報(顧客レコード、単に「レコード」とする場合がある)から、新規取引者である属性情報受信装置50に開示したい属性が選ばれ、属性情報提供サーバ10に対してVIDトークンの発行の依頼がなされる。属性受領者としての任意の相手である属性情報受信装置50は、ユーザ装置30との新規取引の際に、信頼関係構築のための属性証明書を属性情報提供サーバ10経由で受け取っている。

[0027] 属性情報提供サーバ10では、加入者であるユーザ装置30との間でVIDトークンの発行が行われ、また、新規取引者である属性情報受信装置50との間で仮想レコードの参照が行われる。この中で、VIDトークンを秘密にしたまま参照するものをVID秘匿参照とする。尚、属性情報提供サーバ10の機能については、後に詳述する。

[0028] ユーザ装置30では、属性情報提供サーバ10からのVIDトークンの取得と、それを属性情報受信装置50に渡すためのVIDトークンの送信が行われる。

このVIDトークンの取得では、ユーザ装置30は、所定のWebブラウザを使用して属性情報提供サーバ10と通信をする。このとき、SSL(Secure Sockets Layer)などの暗号化および認証機能を用いることによって、第三者が情報を盗み見ることを防ぐことができる。また、ユーザ装置30の認証も、通常のHTTP(Hypertext Transfer Protocol)で定められているBasic認証などを使うことも可能である。

VIDトークンの送信では、ユーザ装置30は、取得したVIDトークンをSMTP(Simple Mail Transfer Protocol)などのメールプロトコルを用いて属性情報受信装置50に送信している。

[0029] 属性情報受信装置50では、ユーザ装置30からのVIDトークンの取得と、属性情報提供サーバ10からの仮想レコードの取得が行われる。

まず、VIDトークンの取得では、通常のメールソフトなどによって、ユーザ装置30からVIDトークンが取得される。

仮想レコードの取得としては、通常取得とVID秘匿取得とがある。通常取得の処理では、VIDトークンに含まれるURLによって属性情報提供サーバ10に接続し、VIDを提示することで、その仮想レコードを取得する。VID秘匿取得では、属性情報受信装置50と属性情報提供サーバ10との間で、後述するOTプロトコルを行うことで、所

定の属性を得ることができる。

[0030] 本実施の形態では、以下の2つの暗号技術を要素技術として用いている。

まず、第1の暗号技術は、オブリビアストランスファー(OT:Oblivious Transfer)である。1-out-of-N OTは、N個の情報を持つサーバと、そのうちの1つを読みたいクライアントの間(2者の間)のプロトコルで、クライアントはN個のうち1つだけ情報を読むことができるが、そのどれを読めたかをサーバは知ることができないとするものである。即ち、情報提供者である属性情報提供サーバ10が持つN個の情報のうち、クライアント(例えば、属性情報受信装置50)は、その1つだけを受け取ることができ、そのどれを選んだかを属性情報提供サーバ10は知り得ない。尚、詳細は文献[Naor, M. and Pinkas, B.: Oblivious Transfer and Polynomial Evaluation, in proc. of STOC, 1999.]に詳しいが、ここではその内容を省略する。

[0031] 第2の暗号技術は、暗号関数の準同型性である。準同型性をもつ公開鍵暗号関数 $E_{pk}(X)$ は、

$$E_{pk1}(E_{pk2}(X)) = E_{pk2}(E_{pk1}(X))$$

を満たす。例えば、後述するエルガマル(ElGamal)暗号などは準同型性を有している。

[0032] ここで、図1に示す属性情報提供システムにて実行される各プロトコルについて説明する。

図2は、属性情報提供システムの各装置が実行する処理を示したフローチャートである。図1の全体構成図を参照して説明すると、まず、ネットワーク70を介してユーザ装置30から属性情報提供サーバ10に対し、仮想ID(VID:VirtualID)を含む仮想IDトークン(VIDトークン)の発行依頼が出される(ステップ201)。このとき、ユーザ装置30は、自分の個人情報(顧客レコード)からどれをVIDトークンの下で開示するかを選択する(ステップ202)。属性情報提供サーバ10では、後述するGID(Globally-unique ID)から属性の一部がコピーされ、仮想IDをキーとしてデータベース(後述)に登録される(ステップ203)。そして、属性情報提供サーバ10からユーザ装置30に対して、ネットワーク70を介してVIDトークンが発行される(ステップ204)。

[0033] その後、ユーザ装置30から属性情報受信装置50に対し、VIDトークンが渡され、

仮想IDを含めた取引依頼がネットワーク70を介して出力される(ステップ205)。その後、属性情報受信装置50は、属性情報提供サーバ10に対して取得した仮想IDを提示し、付随する属性情報の開示を要求する(ステップ206)。属性情報提供サーバ10は、仮想IDをキーとする属性を与信情報として、即ち、仮想IDの参照情報(仮想レコード)を属性情報受信装置50に開示する(ステップ207)。このようにして、仮想レコードを取得した属性情報受信装置50は、開示された属性(仮想レコードの結果)により、新規取引するだけの信頼が得られた場合には、ユーザ装置30に対してネットワーク70を介し、取り引きの承諾を通知し、ユーザ装置30と属性情報受信装置50との間で取り引きが開始される(ステップ208)。

[0034] 次に、本実施の形態が適用される各構成要素のハードウェア構成について説明する。

図3は、本実施形態の属性情報提供サーバ10やユーザ装置30、属性情報受信装置50を実現するのに好適なコンピュータ装置のハードウェア構成例を模式的に示した図である。

図3に示すコンピュータ装置は、演算手段であるCPU(Central Processing Unit: 中央処理装置)101、M/B(マザーボード)チップセット102、このM/Bチップセット102およびCPUバスを介してCPU101に接続されたメインメモリ103、同じくM/Bチップセット102およびAGP(Accelerated Graphics Port)を介してCPU101に接続されたビデオカード104を備えている。また、PCI(Peripheral Component Interconnect)バスを介してM/Bチップセット102に接続された磁気ディスク装置(HDD)105、およびネットワークインターフェイス106を有している。更に、このPCIバスからブリッジ回路107およびISA(Industry Standard Architecture)バスなどの低速なバスを介してM/Bチップセット102に接続されたフロッピーディスクドライブ108、およびキーボード/マウス109とを備えている。

[0035] 尚、図3は本実施形態を実現するコンピュータ装置のハードウェア構成を例示するに過ぎず、本実施形態を適用可能であれば、他の種々の構成を取ることができる。例えば、ビデオカード104を設ける代わりに、ビデオメモリのみを搭載し、CPU101にてイメージデータを処理する構成としても良い。また、外部記憶装置として、ATA(AT

Attachment)やSCSI(Small Computer System Interface)などのインターフェイスを介して、CD-R(Compact Disc Recordable)やDVD-RAM(Digital Versatile Disc Random Access Memory)のドライブ等を設けることも可能である。

[0036] 次に、本実施形態の属性情報提供サーバ10における機能構成を、図4を用いて詳述する。

図4に示すように、属性情報提供サーバ10は、VID発行の機能として、抜き出し指示を受ける手段として機能する顧客レコード表示部11および属性選択部12、仮想レコードの生成手段の一つとして機能する仮想レコード生成部13、仮想ID提供手段の一つとして機能するVIDトークン発行部14を備えている。また、仮想レコードの参照機能(仮想レコード提供手段)として、仮想レコード参照処理部18および仮想レコード発行部19を備えている。更に、例えば図3に示す磁気ディスク装置105を用いて、加入者であるユーザ装置30の顧客レコードや仮想レコードを格納するデータベース20を備えている。

[0037] このデータベース20では、図5に示すようなテーブルで個人情報を管理している。もともとの個人情報のレコードは、顧客ごとに、複数の属性からなる顧客レコードをGID(Globally-unique ID)をキーとして保存されている。そして、ここから属性の一部がコピーされたものを、仮想IDをキーとして登録するものとしている。図5に示すように、同一個人の情報であっても、仮想IDでは、GIDの属性の異なった一部だけがコピーされており、仮想IDである「V010101」と「V010011」とでは、各々、異なった属性情報が選択されている。仮想ID属性の属性証明では、不必要な属性にはフィルタがかけられている。また、例えば図5に示す仮想ID「V010011」のように、匿名属性として、名前の部分にフィルタをかけることができる。仮想IDの発行に際し、この仮想IDは、GIDとはアンリンクابل(Unlinkable)なIDとされる。また、属性コピーでは、必要な属性のみが実IDであるGIDの属性からコピーされる。尚、仮想IDフィールドは、実IDと全く同等に扱うことができ、属性が欠落した実IDレコードとの区別がつかないように構成されている。

[0038] 顧客レコード表示部11は、仮想IDの発行に際し、データベース20より加入者であるユーザ装置30の顧客レコードを取り出し、この取り出した内容を、参照のために、

例えばユーザ装置30のディスプレイ(図示せず)に表示する。ここで表示される顧客レコードは、例えば、図5に示したように、プライマリーキーとしてGIDを持ち、名前や住所などの複数の属性からなるレコードである。尚、顧客レコード表示部11には、図5に示すように、GIDと共に、今までに所定の属性が選択されて生成された仮想レコードも表示させ、参照させることができる。

属性選択部12は、加入者であるユーザ装置30に、表示された属性から、新規取引者である属性情報受信装置50に提示したい属性だけを抜き出させる(選ばせる)。

- [0039] 仮想レコード生成部13は、ユーザ装置30にて抜き出された属性だけをコピーした新しいレコードを作る。このレコードのプライマリーキーとして、既存のレコードのプライマリーキーであるGIDとぶつからないようなIDを生成し、これを仮想IDとする。また、ここでは、仮想IDの値が定義されるドメインは、十分に大きいものとし、仮想IDを知らない者が総当たり攻撃などで偶然、仮想IDを探りあててことはないものと仮定する。生成された仮想レコードは、データベース20に格納される。

VIDトークン発行部14では、仮想レコード生成部13によって生成された仮想IDと、自サーバ(属性情報提供サーバ10)のURLの組{VID,URL}とをVIDトークンとして発行する。

- [0040] 仮想レコード参照処理部18では、仮想レコードの参照に際して、通常参照の処理、またはVID秘匿参照の処理が実行される。VIDトークンをユーザ装置30から受信した属性情報受信装置50は、前述のように、例えばブラウザを用いて、VIDトークンに含まれるURLにアクセスすることにより、属性情報提供サーバ10に接続される。仮想レコード参照処理部18は、属性情報受信装置50から提示された仮想IDに基づいて、データベース20から仮想レコードを検索し、仮想レコード発行部19により、属性情報受信装置50のディスプレイ(図示せず)に検索結果を表示する。属性情報受信装置50は、かかる表示によって、仮想レコードにある属性情報を取得することができる。場合によっては、仮想レコード参照処理部18や仮想レコード発行部19にて、属性に属性情報提供サーバ10の署名を付けて、確かに属性情報提供サーバ10にある属性情報であるということを証明するようなサービスも付加することが可能である。

- [0041] 次に、属性情報提供サーバ10にて実行される仮想ID秘匿参照の処理について説

明する。

秘匿参照は、仮想IDを属性情報提供サーバ10に秘密にしたまま仮想レコードを取得するものであり、前述したOT(Oblivious Transfer)が用いられる。以下では簡単なOT、

OT($\{s_1, \dots, s_n\}$)について説明する。

まず、属性情報提供サーバ10は、予めランダムに秘密の値 $t_s \in \mathbb{Z}_q$ を決定し

$$Q_0 = g^{t_s} \pmod{p}$$

を公開しておく。

属性情報受信装置50は、秘密鍵 t_u をランダムに \mathbb{Z}_q から選び、その公開鍵である

$$Q_u = g^{t_u} \pmod{p}$$

を計算する。ここで、属性情報受信装置50は、属性情報提供サーバ10の h 番目の情報を得ようとしているものとする。このとき、まず、2点 $\{(0, Q_0), (h, Q_u)\}$ を通るような1次多項式 $Y(x)$ を、例えばラグランジュの補間法を使って一意に決定する。この多項式を使って、 n 点 $Y_i = Y(i), i=0, \dots, n-1$ を計算し、 $\{Y_1, Y_2, \dots, Y_n\}$ を属性情報提供サーバ10に送る。

属性情報提供サーバ10は、属性情報受信装置50の公開している点が1次多項式上の点であることを検証した後、 Y_i をそれぞれエルガマル(ElGamal)暗号の公開鍵として、秘密情報 s_i を暗号化したもの $E_{Y_i}(s_i)$, $i=1, \dots, n$ を属性情報受信装置50に送る。

属性情報受信装置50は、 h によって指定された点については、それに対応する秘密鍵 t_u を持っているので、属性情報提供サーバ10から送り返されたElGamal暗号文を復号できる。したがって、1個の秘密情報を得ることが可能となる。

[0042] OTでは、 h 番目を指定しなければならないが、属性情報受信装置50の持つ仮想ID(VID)が、全体の顧客レコードの何番目であるのかは、以下のように設定することができる。例えば、属性情報提供サーバ10は、一方向性ハッシュ関数 $H()$ を用い、 $H(\text{VID})$ のリストを公開することで設定を可能とすることができる。ここで、ハッシュ関数 H

のアルゴリズムは公開されているものとする。また、例えば、新規取引業者である属性情報受信装置50は、H(VID)のリスト中で自分の持つ仮想IDが何番目であるかを知ることができる。

- [0043] これで、上記のOTプロトコルによって、H(VID)番目のレコードを取得することができる。但し、このままでは、自分の持っている仮想IDに対応するH(VID)番目以外を指定してくることがあり、これを防ぐためには、別のハッシュ関数 H' を用い、予め仮想レコードの属性を $H'(VID)$ を鍵として暗号化しておく。このハッシュ関数 H' のアルゴリズムも公開されているものとする。まとめると以下のように構成される。

例えば、仮想レコードが以下のように m 個の属性からなっていたとする。

$$\{VID_i, Attr_{i,1}, \dots, Attr_{i,m}\}$$

これを $k_i = H'(VID_i)$ として、属性を暗号化して以下のようにする。

$$s_i = \{H(VID_i), E_{k_i}(Attr_{m1}), \dots, E_{k_i}(Attr_m)\}$$

そして、 $H(VID_i)$ をキーとして、仮想レコード全体をソートし、順番を割り振り、これに対して $OT(\{s_1, \dots, s_n\})$ を行えばよい。

属性情報受信装置50では、例えば、ユーザ装置30から得た仮想IDに基づいて、仮想レコード

$$s_i = \{H(VID_i), E_{k_i}(Attr_{m1}), \dots, E_{k_i}(Attr_m)\}$$

を取得することができる。これを $k_i = H'(VID_i)$ によって復号することによって、 m 個の属性を得ることができる。

- [0044] 以上、詳述したように、本実施の形態では、まず、加入者であるユーザ装置30は、所定のブラウザを用い、ネットワーク70を介して個人情報取り扱い業者の運営する属性情報提供サーバ10に入るように構成した。そして、属性情報提供サーバ10上のデータベース20に格納された個人属性テーブルから、必要情報だけを抜き出したものを仮想レコードとして登録し、このキーとして仮想IDを発行してもらうように構成した。その後、ユーザ装置30は仮想IDと認証に必要な情報とを新規取引業者である属性情報受信装置50に送り、属性情報受信装置50では、その仮想IDを使って、属性情報提供サーバ10にログインしている。そして、属性情報受信装置50は、仮想レコードに登録された情報データを属性情報提供サーバ10から得ることで、属性データ

を参照し、取引相手が信頼できるかを判断して、取引を開始することが可能となる。

[0045] 尚、このプロトコルにおけるセキュリティの要件として、

- (1) ユーザ装置30は、属性情報提供サーバ10上の自分の属性レコードだけを読むことができる。
- (2) ユーザ装置30は、仮想レコードを登録する際に、元の属性レコード(GIDレコード)の中の任意の属性をコピーすることはできるが、改ざんすることはできない。
- (3) 属性情報受信装置50は、属性情報提供サーバ10から渡された仮想ID(+パスワード)によって、その仮想レコードだけを読むことができる。また、このとき次のプライバシー要件も必要に応じて付加することができる。
- (4) 属性情報提供サーバ10は、属性情報受信装置50が仮想レコードを取得するときに、それがどの仮想IDなのか、即ち、どのユーザ装置30の仮想レコードを渡そうとしているのかを知ることができない(知り得ない)。としている。

上記要件の(1)および(3)は、従来の認証の仕組みを使えば容易に実現される。上記要件の(2)については、次のように仮想レコード登録時のサーバ側のチェックとして実現することが可能である。

[0046] また、上述したように、本実施の形態では、属性情報提供サーバ10上での仮想レコードおよび仮想IDの発行は、以下のようになされる。

- (1) 個人情報レコードは、GIDというIDをプライマリーキーとして、データベース20上に登録されているものとする。
- (2) 加入者であるユーザ装置30は、GIDとは無関係な仮想ID(VID)をキーとする空のレコードを作る。
- (3) 加入者であるユーザ装置30は、自分のGIDレコードのうち、取引相手(属性情報受信装置50)に開示したい属性部分だけを仮想IDのレコードにコピーする。
- (4) このとき、属性情報提供サーバ10は、オリジナルのレコードの属性部と仮想レコードの属性部のORを計算し、この結果がオリジナルレコードの属性部と等しいことを検証する。即ち、

$$\text{Attribute(GID) OR Attribute(VID) = Attribute(GID)}$$

また、この要件(4)については、暗号技術OTによって実現される。

[0047] 以上のような構成によって、本実施の形態では、個人情報を持つ機関(属性情報提供サーバ10)が、その個人の求めに応じて、個人情報の一部を第三者に提供しており、この個人情報を持つ機関は、それを提供するビジネス展開が可能となる。また、加入者(ユーザ装置30)は、インターネット(ネットワーク70)上で必要な与信を簡単に得ることができる。個人情報を持つ機関(属性情報提供サーバ10)としては、金融機関やISP(Internet Service Provider)、ネット上の商店サイト等でもよく、加入者(ユーザ装置30)の同意の下に個人情報を発行するので、プライバシーの問題も生じない。また、新規取引業者(属性情報受信装置50)が、渡された情報を十分な与信情報と見るか否かは、新規取引業者(属性情報受信装置50)の任意である。更に、個人情報取り扱い業者(属性情報提供サーバ10)は、開示する情報については、それが自らが持つ情報と同等である(改ざんされていない)ことだけが責任範囲となり、与信情報そのものについての正当性の保障をする必要がない。例えば、加入者(ユーザ装置30)が自分の情報の登録時に虚偽の情報を登録した場合の正当性の保証をするものではない。

[0048] また、本実施の形態によれば、属性レコード自体が、加入者(ユーザ装置30)と個人情報取り扱い業者(属性情報提供サーバ10)の共有物(加入者自身が登録した属性と、預金額などの活動履歴情報)であることから、加入者(ユーザ装置30)は、属性情報提供サーバ10上の自分の属性レコードだけを読むことができる。また、加入者(ユーザ装置30)は、仮想レコードを登録する際に、元の属性レコードの中における任意の属性をコピーすることはできるが、改ざんすることはできない。これによって、加入者は、名前を特定されずに預金額などの属性だけを証明することが可能となる。更に、新規取引業者(属性情報受信装置50)は、加入者(ユーザ装置30)から渡された仮想ID(+パスワード)によって、その仮想レコードだけを読むことができる。即ち、新規取引業者(属性情報受信装置50)側にて認証は仮想IDだけで行われるので、個人情報取り扱い業者(属性情報提供サーバ10)は、だれが仮想レコードをアクセスしたかを知ることができない。その結果、この仮想IDの受け渡しは、加入者(ユーザ装置30)の責任であることが明確化される。また更に、個人情報取り扱い業者(属性情報提供サーバ10)は、1-out-of-N OTによって、どの加入者(ユーザ装置30)の仮想IDを要求されて

いるのかを知り得ない。これによって、加入者(ユーザ装置30)は、自分がどの新規取引業者(属性情報受信装置50)と取引しようとしているかを、個人情報取り扱い業者(属性情報提供サーバ10)に知られない状態で、認証だけを受けることができる。これによって、加入者(ユーザ装置30)のプライバシーの保護が強化され、また、個人情報取引業者(属性情報提供サーバ10)にとっても、不必要な情報を知ることなく、サービスすることが可能となる。

産業上の利用可能性

- [0049] 本発明の活用例としては、属性情報提供サーバとして用いられるサーバ、ユーザ装置や属性情報受信装置として用いられるPCなどのコンピュータ装置などがあり、これらをインターネットなどのネットワークを介してWeb接続されたシステム構成が考えられる。サービスプロバイダとして適用される属性情報提供サーバは、ISP(Internet Service Provider)や金融機関、ショップサイトなどが考えられる。サービスプロバイダとしての社会的信頼が高ければ高いほど、その与信サービスも価値あるものとなる。

図面の簡単な説明

- [0050] [図1]本実施の形態が適用される属性情報提供システム(与信付与システム)の全体構成を示した図である。
- [図2]属性情報提供システムの各装置が実行する処理を示したフローチャートである。
- [図3]本実施形態の属性情報提供サーバやユーザ装置、属性情報受信装置を実現するのに好適なコンピュータ装置のハードウェア構成例を模式的に示した図である。
- [図4]本実施形態の属性情報提供サーバにおける機能構成を示した図である。
- [図5]ユーザ装置のディスプレイに表示される顧客記録および仮想記録の例を示した図である。

符号の説明

- [0051] 10…属性情報提供サーバ(個人情報サーバ)、11…顧客記録表示部、12…属性選択部、13…仮想記録生成部、14…VIDトークン発行部、18…仮想記録参照処理部、19…仮想記録発行部、20…データベース、30…ユーザ装置、50…属性情報受信装置(与信情報受信装置)、70…ネットワーク

請求の範囲

- [1] 属性情報が格納されたデータベースから所定の属性情報をネットワークを介して提供する属性情報提供サーバであって、
- ネットワークを介して接続されるユーザ装置により、データベースに格納されている属性情報の中から幾つかの属性情報の抜き出し指示を受ける手段と、
- 前記ユーザ装置によって指示されデータベースから抜き出された前記幾つかの属性情報だけを仮想レコードとしてデータベースに登録する手段と、
- 前記仮想レコードのキーとしての仮想IDを前記ユーザ装置に提供する手段と、
- ネットワークを介して接続される属性情報受信装置から、前記仮想IDを用いた前記仮想レコードの読み込み要求を受ける手段と、
- 前記属性情報受信装置に対して前記仮想レコードを提供する手段とを含む属性情報提供サーバ。
- [2] 前記抜き出し指示を受ける手段は、前記ユーザ装置だけに当該ユーザ装置の操作者に関する属性情報を参照させ、前記仮想レコードを抜き出させる際に、任意の属性に対するコピーを許可する一方、任意の属性に対する改ざんを禁止することを特徴とする請求項1記載の属性情報提供サーバ。
- [3] 前記読み込み要求を受ける手段は、データベースの中からどの仮想IDに対する仮想レコードの読み込み要求がなされているかを知り得ない状態にあることを特徴とする請求項1記載の属性情報提供サーバ。
- [4] データベースに格納される属性情報の中から選択された所定の情報である仮想レコードを生成する生成手段と、
- 前記仮想レコードのキーとなる仮想IDに対応付けてデータベースに格納する格納手段と、
- ネットワークを介して接続されるユーザ装置に前記仮想IDを提供する仮想ID提供手段と、
- ネットワークを介して接続される属性情報受信装置からの前記仮想IDを用いた要求に基づいて、当該属性情報受信装置に前記仮想レコードを提供する仮想レコード提供手段とを含み、

前記仮想レコード提供手段は、データベースの中からどの仮想IDが選ばれたかを
知り得ない状態にて、当該属性情報受信装置に前記仮想レコードを提供することを
特徴とする属性情報提供サーバ。

[5] 前記生成手段は、データベースに格納されている加入者の属性情報の中から、前
記ユーザ装置によって抜き出された情報を仮想レコードとして生成することを特徴と
する請求項4記載の属性情報提供サーバ。

[6] 前記仮想レコード提供手段は、1-out-of-N OT(Oblivious Transfer)のプロトコルを
用いて、前記属性情報受信装置に前記仮想レコードを提供することを特徴とする請
求項4記載の属性情報提供サーバ。

[7] 顧客ごとに、複数の属性情報を含む顧客レコードを格納するデータベースと、
顧客が操作するユーザ装置からの要求に基づき、前記データベースから当該顧客
の顧客レコードを読み出し、ネットワークを介して前記ユーザ装置に提供する顧客レ
コード表示部と、

前記ユーザ装置からネットワークを介し、前記顧客レコードの中から所定の属性情
報に対する選択を受ける属性選択部と、

前記属性選択部により受けた選択に基づき、前記顧客レコードの中から選択された
属性情報によって仮想レコードを生成すると共に、生成された当該仮想レコードを前
記データベースに格納する仮想レコード生成部と、

前記仮想レコード生成部により生成された前記仮想レコードを特定するための仮想
IDを前記ユーザ装置に提供する仮想ID発行部とを含む属性情報提供サーバ。

[8] 属性情報受信装置からネットワークを介してなされる前記仮想IDを用いた情報参
照要求に基づき、前記データベースから該当する仮想レコードを読み出して当該属
性情報受信装置に提供する仮想レコード参照処理部を更に備えたことを特徴とする
請求項7記載の属性情報提供サーバ。

[9] 前記仮想レコード生成部は、オリジナルである前記顧客レコードの属性内容と、生
成された前記仮想レコードの属性内容とを比較し、改ざんされていないことを検証す
ることを特徴とする請求項7記載の属性情報提供サーバ。

[10] 前記仮想ID発行部により前記ユーザ装置に提供される前記仮想IDは、前記顧客

レコードのIDとはアンリンカブルなIDであることを特徴とする請求項7記載の属性情報提供サーバ。

- [11] 複数の属性情報を含むレコードを格納するレコード格納手段と、
前記レコード格納手段により格納された前記レコードの中から、ネットワークを介して選択された所定の属性情報によって生成された仮想レコードを格納する仮想レコード格納手段と、
どの仮想レコードが選ばれたかを知り得ない状態にて、前記仮想レコード格納手段の中から選ばれた仮想レコードを、ネットワークを介して開示する仮想レコード開示手段とを含む属性情報提供サーバ。
- [12] 前記仮想レコード格納手段は、キーとしての仮想IDに対応付けて仮想レコードを格納し、
前記仮想レコード開示手段は、どの仮想IDが選ばれたかを知り得ない状態にて、前記仮想IDを用いた開示要求を受けることを特徴とする請求項11記載の属性情報提供サーバ。
- [13] 前記仮想レコード開示手段は、オブリビアストランスファー(Oblivious Transfer)の暗号技術を用いて前記仮想レコードの開示を実現することを特徴とする請求項11記載の属性情報提供サーバ。
- [14] ネットワークを介してなされたユーザ装置からの要求に基づき、複数の属性情報からなるレコードが格納されたデータベースから、所定のレコードを読み出すステップと、
読み出された前記所定のレコードを、ネットワークを介して前記ユーザ装置に提供するステップと、
前記所定のレコードの中から所定の属性情報に対する前記ユーザ装置からの選択をネットワークを介して受けるステップと、
前記所定のレコードの中から選択された前記所定の属性情報を含む仮想レコードを生成するステップと、
生成された前記仮想レコードをデータベースに格納するステップと、
格納された前記仮想レコードを特定するための仮想IDをネットワークを介して前記

- ユーザ装置に提供するステップとを含む属性情報提供方法。
- [15] ネットワークを介して属性情報受信装置から前記仮想IDを用いた情報参照要求を受けるステップと、
前記情報参照要求に基づき、データベースから該当する仮想レコードを読み出すステップと、
読み出された前記仮想レコードを前記属性情報受信装置にネットワークを介して提供するステップとを更に含む請求項14記載の属性情報提供方法。
- [16] 前記情報参照要求は、1-out-of-N OT(Oblivious Transfer)の protokolを用いてなさ
れることを特徴とする請求項14記載の属性情報提供方法。
- [17] データベースに格納される前記仮想レコードの属性情報が前記顧客レコードの属性情報から改ざんされたものでないことを検証するステップを更に含む請求項14記載の属性情報提供方法。
- [18] 顧客別の顧客レコードの中から所定の属性が選択されて生成された仮想レコードをキーとなる仮想IDに対応付けて格納されたデータベースに対して、当該仮想IDを用いた当該仮想レコードの取得要求を受けるステップと、
前記仮想IDに対応する前記仮想レコードを前記データベースから読み出し、前記取得要求に対して当該仮想レコードを開示するステップとを含み、
前記仮想レコードの取得要求を受けるステップは、当該取得要求を受ける際に、どの仮想IDが選ばれたかが秘匿されることを特徴とする属性情報提供方法。
- [19] 顧客自身のコンピュータ装置を介して、当該顧客自身の顧客レコードの中から所定の属性の選択を受けるステップと、
選択された前記所定の属性だけを属性とする前記仮想レコードを生成して前記データベースに格納するステップと、
前記データベースに格納された前記仮想レコードのキーとなる前記仮想IDを前記コンピュータ装置に提供するステップとを更に含む請求項18記載の属性情報提供方法。
- [20] ネットワークを介して属性情報を提供するための属性情報提供サーバとして機能す

るコンピュータに、

ネットワークを介してなされたユーザ装置からの要求に基づき、複数の属性情報からなるレコードが格納されたデータベースから、所定のレコードを読み出す機能と、
読み出された前記所定のレコードを、ネットワークを介して前記ユーザ装置に提供する機能と、

前記所定のレコードの中から所定の属性情報に対する前記ユーザ装置からの選択をネットワークを介して受ける機能と、

前記所定のレコードの中から選択された前記所定の属性情報を含む仮想レコードを生成する機能と、

生成された前記仮想レコードをデータベースに格納する機能と、

格納された前記仮想レコードを特定するための仮想IDをネットワークを介して前記ユーザ装置に提供する機能とを実現させるプログラム。

[21] 前記コンピュータに、データベースに格納される前記仮想レコードの属性情報が前記レコードの属性情報から改ざんされたものではないことを検証する機能を更に実現させる請求項20記載のプログラム。

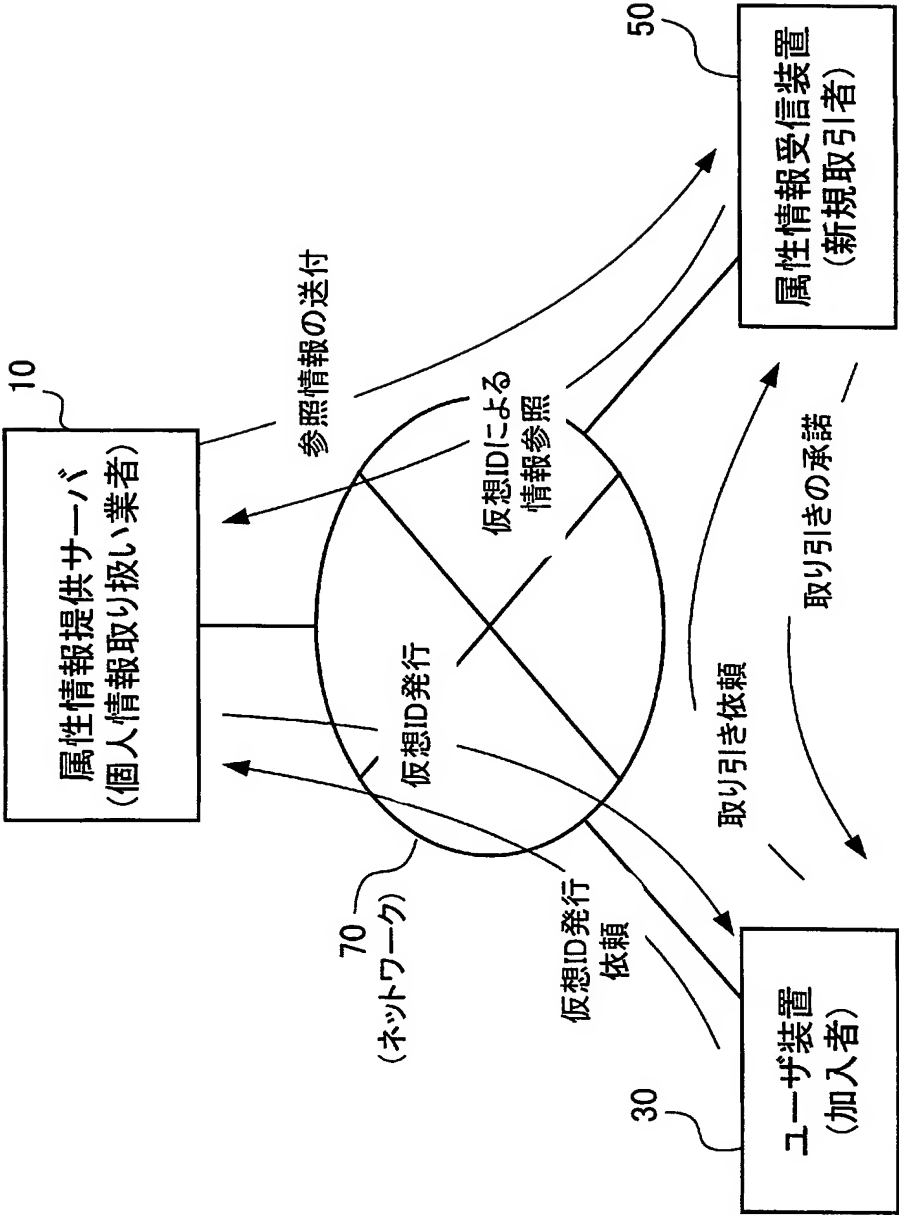
[22] ネットワークを介して属性情報を提供するための属性情報提供サーバとして機能するコンピュータに、

格納されるレコードの中から所定の属性が選択されて生成された仮想レコードを、キーとなる仮想IDに対応付けてデータベースに格納する機能と、

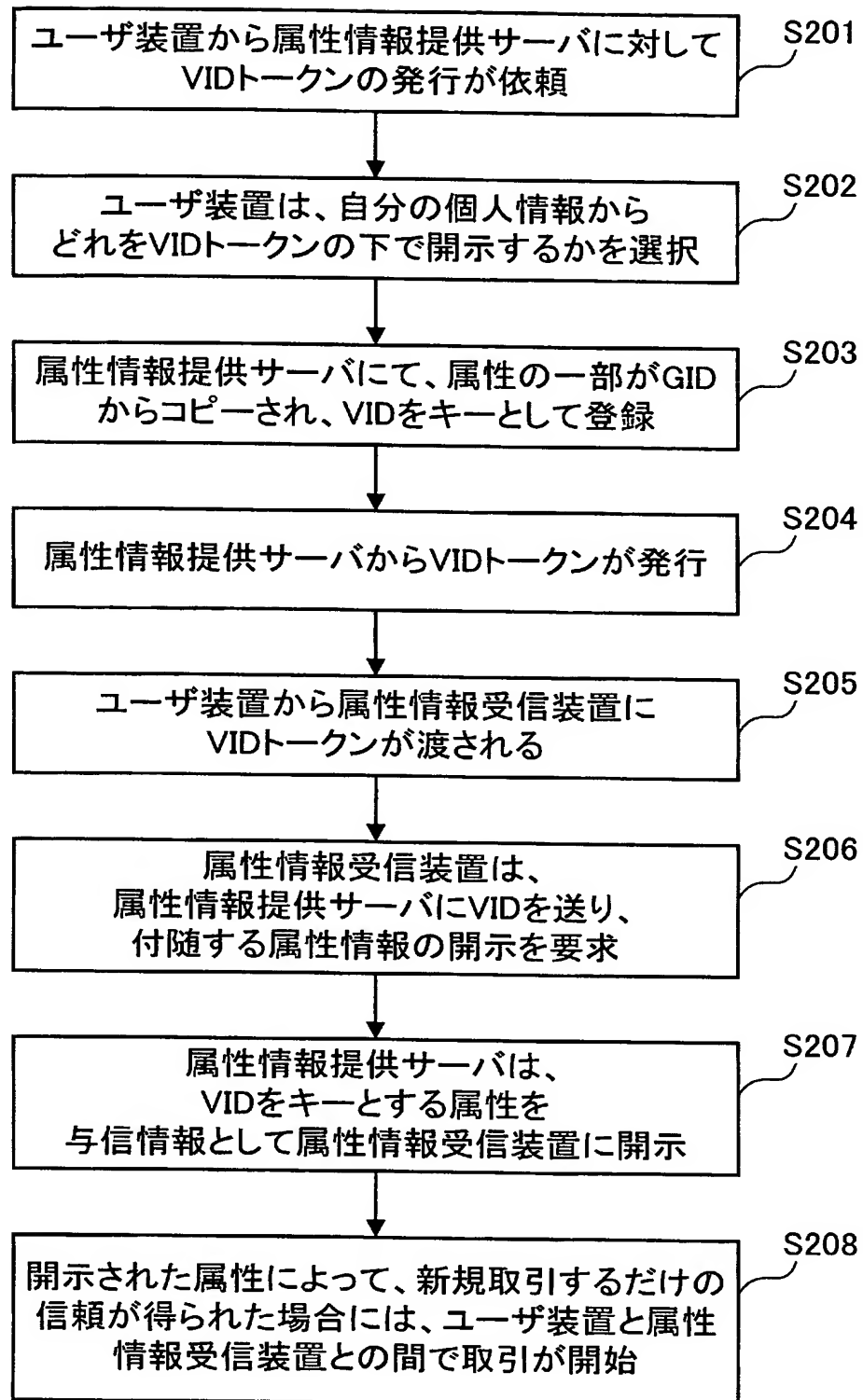
どの仮想IDが選ばれたかが秘匿された状態にて前記仮想IDを用いた前記仮想レコードの取得要求を受ける機能と、

前記仮想IDに対応する前記仮想レコードを前記データベースから読み出し、前記取得要求に対して当該仮想レコードを開示する機能とを実現させるプログラム。

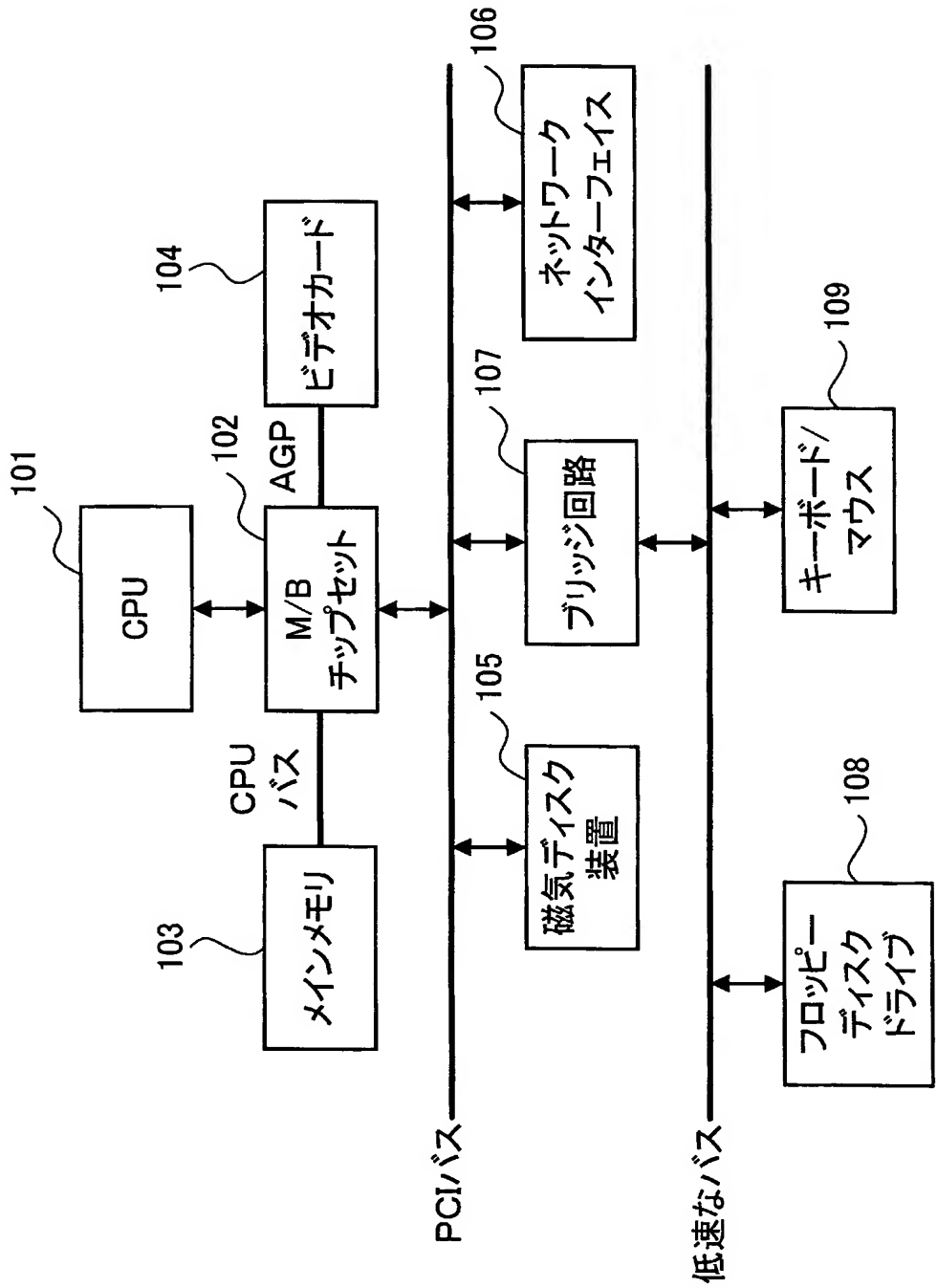
[図1]



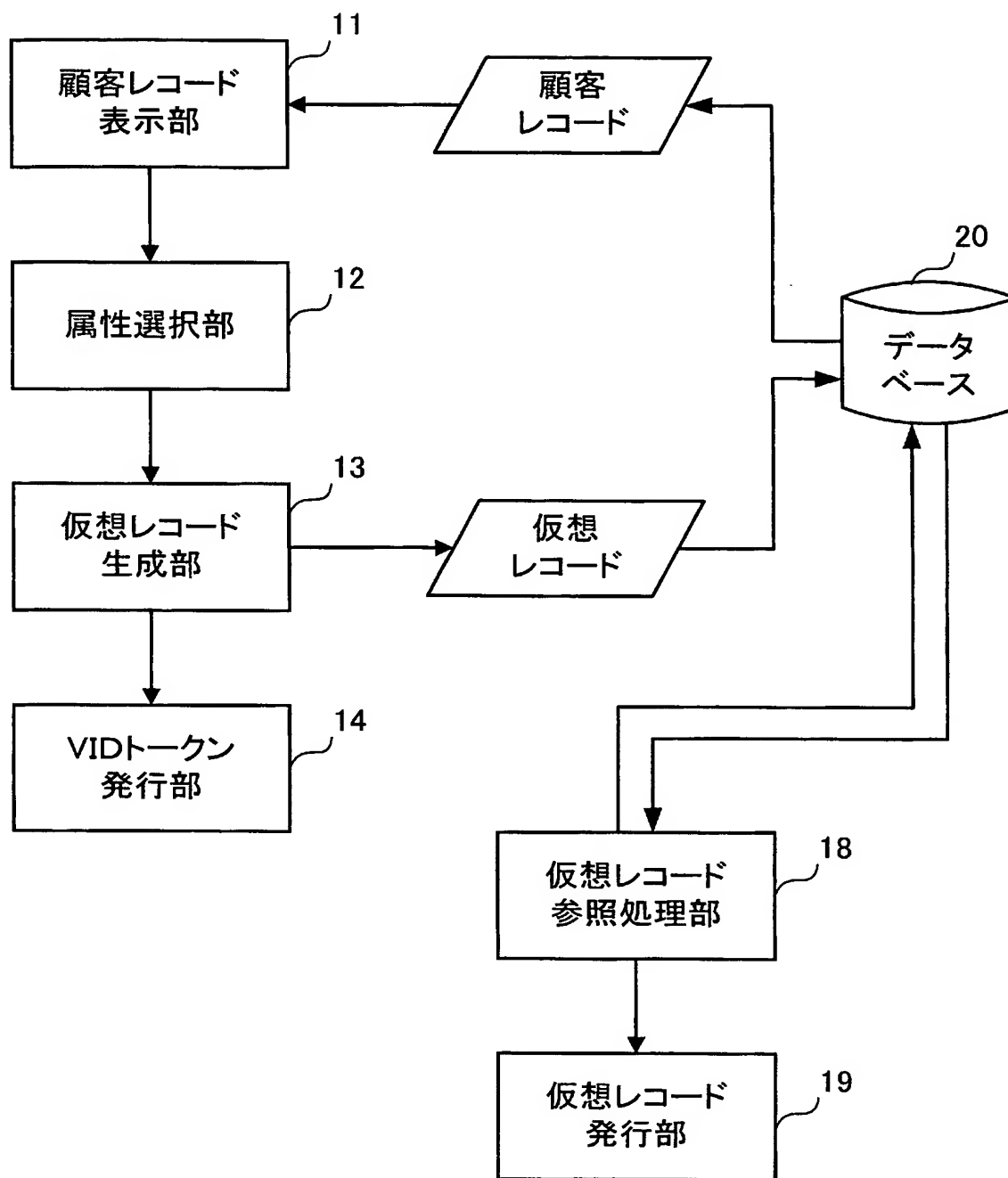
[図2]



[図3]



[図4]



[図5]

GID/VID	名前	口座番号	住所	電話番号	預金残高	...
G000011	鈴木一郎	123456	東京都	333-4444	1,000,000	
V010101	鈴木一郎	-	-	-	1,000,000	
V010011	-	-	東京都	-	1,000,000	

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2004/011831

A. CLASSIFICATION OF SUBJECT MATTER

Int.Cl⁷ G06F17/60

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

Int.Cl⁷ G06F17/60

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Jitsuyo Shinan Koho 1922-1996 Toroku Jitsuyo Shinan Koho 1994-2004

Kokai Jitsuyo Shinan Koho 1971-2004 Jitsuyo Shinan Toroku Koho 1996-2004

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	JP 2002-203109 A (Kabushiki Kaisha CIC), 19 July, 2002 (19.07.02) < Full text; Figs. 1 to 9 & US 2002/0087553 A1	1-22
A	JP 2002-366730 A (Hitachi, Ltd.), 20 December, 2002 (20.12.02), Full text; Figs. 1 to 7 (Family: none)	1-22
A	JP 11-149504 A (Hitachi, Ltd.), 02 June, 1999 (02.06.99), Full text; Figs. 1 to 43 & US 2002/0162006 A1	1-22

☒ Further documents are listed in the continuation of Box C.

☐ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search
14 October, 2004 (14.10.04)

Date of mailing of the international search report
02 November, 2004 (02.11.04)

Name and mailing address of the ISA/
Japanese Patent Office

Authorized officer

Facsimile No.

Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2004/011831

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	JP 2003-150725 A (Yugen Kaisha Business System Design), 23 May, 2003 (23.05.03), Full text; Figs. 1 to 17 (Family: none)	1-22
A	JP 2002-082955 A (Datto Japan Kabushiki Kaisha), 22 March, 2002 (22.03.02), Full text; Figs. 1 to 13 & US 2002/0087539 A1	1-22

A. 発明の属する分野の分類 (国際特許分類 (IPC))

Int. Cl⁷ G06F17/60

B. 調査を行った分野

調査を行った最小限資料 (国際特許分類 (IPC))

Int. Cl⁷ G06F17/60

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報	1922-1996年
日本国公開実用新案公報	1971-2004年
日本国登録実用新案公報	1994-2004年
日本国実用新案登録公報	1996-2004年

国際調査で使用した電子データベース (データベースの名称、調査に使用した用語)

C. 関連すると認められる文献

引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
X	J P 2002-203109 A (株式会社シー・アイ・シー) 2002.07.19, 全文, 第1-9図 & US 2002/ 0087553 A1	1-22
A	J P 2002-366730 A (株式会社日立製作所) 200 2.12.20, 全文, 第1-7図 (ファミリーなし)	1-22
A	J P 11-149504 A (株式会社日立製作所) 1999. 06.02, 全文, 第1-43図 & US 2002/0162 006 A1	1-22

☒ C欄の続きにも文献が列挙されている。☐ パテントファミリーに関する別紙を参照。

* 引用文献のカテゴリー

「A」 特に関連のある文献ではなく、一般的技術水準を示すもの
「E」 国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
「L」 優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献 (理由を付す)
「O」 口頭による開示、使用、展示等に言及する文献
「P」 国際出願日前で、かつ優先権の主張の基礎となる出願

の日の後に公表された文献
「T」 国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
「X」 特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
「Y」 特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
「&」 同一パテントファミリー文献

国際調査を完了した日

14.10.2004

国際調査報告の発送日

02.11.2004

国際調査機関の名称及びあて先

日本国特許庁 (ISA/J P)

郵便番号100-8915

東京都千代田区霞が関三丁目4番3号

特許庁審査官 (権限のある職員)

石川 正二

5 L

3136

電話番号 03-3581-1101 内線 3560

C (続き) . 関連すると認められる文献		
引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
A	J P 2003-150725 A (有限会社ビジネスシステムデザイン) 2003. 05. 23, 全文, 第1-17図 (ファミリーなし)	1-22
A	J P 2002-082955 A (ダットジャパン株式会社) 2002. 03. 22, 全文, 第1-13図 & US 2002/0087539 A1	1-22